Die Zerlegung der Lagrange'schen Resolventen für die Kreisteilungsgleichungen in ihre Primfaktoren.

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

der

Hohen philosophischen Fakultät der Universität Marburg

vorgelegt von

Paul Berger
aus Krefeld (Rheinland).

ACAD.
LUGD.BAT.
BIBL.

Marburg.
R. Friedrich's Universitäts-Buchdruckerei (Inhaber: Karl Gleiser).
1914.

Von der Fakultät als Dissertation angenommen
am 31. Mai 1913.

Referent: Herr Geh. Reg.-Rat Prof. Dr. Hensel.

Inhaltsverzeichnis.

Einleitung.

Abschnitt I. Die Resolvente der Gleichung $x^p - 1 = 0$.

§ 1. Der Körper $K(p, \omega)$.

§ 2. Der Körper $K(p, \varepsilon)$.

§ 3. Der Körper $K(p, \omega, \varepsilon)$.

§ 4. (ε, ω) ist genau durch $\mathfrak{P}_1^{p-2}$ teilbar.

§ 5. Das Resultat: $(\varepsilon, \omega) = \prod_{h=1}^{\varphi(p-1)} \mathfrak{P}_h^{p-1-a_h}$.

§ 6. Die von Kummer behandelte Resolvente.

Abschnitt II. Die Resolvente der Gleichung $x^{p^\nu} - 1 = 0$.

§ 1. Der Körper $K(p, \omega)$.

§ 2. Der Körper $K(p, \varepsilon)$.

§ 3. Der Körper $K(p, \varepsilon, \omega)$.

§ 4. (ε_1, ω) als π-adische Zahl.

§ 5. (ε_1, ω) als Summe von $(p-1)$ π-adische Zahlen:

$$(\varepsilon_1, \omega) = \sum_{i=1}^{p-1} C_i \, a_1^{k_i}.$$

§ 6. Das nicht verschwindende C_1.

§ 7. Die verschwindenden C_i.

§ 8. Die Entwicklung von $(\varepsilon_1^{-1}, \omega)$.

§ 9. (ε_1, ω) und $(\varepsilon_1^{-1}, \omega)$ enthalten dieselbe Potenz von π.

§ 10. (ε, ω) enthält die Potenz $\mathfrak{P}_1^{\nu \cdot \frac{\varphi_\nu}{2}}$.

§ 11. Das Resultat.

Abschnitt III. Die Resolvente der Gleichung $x^{2^\nu} - 1 = 0$.

§ 1. Der Körper $K(2, \omega)$.

§ 2. Der Körper $K(2, \varepsilon, \omega)$.

§ 3. Die π-adische Entwicklung von $(-1, \varepsilon_1, \omega)$.

§ 4. Reduktion der π-adischen Entwicklung von $(-1, \varepsilon_1, \omega)$.

§ 5. Der Ausdruck $(-1, \varepsilon_1^{-1}, \omega)$.

§ 6. Das Resultat.

Abschnitt IV. Die Resolvente der Gleichung $x^m - 1 = 0$.

Einleitung.

Die vorliegende Arbeit behandelt die Primteilerzerlegung der Lagrange'schen Resolventen für die Kreisteilungsgleichungen, und zwar auf Grund der Hensel'schen Theorie der algebraischen Zahlen. Massgebend für die Stellung des Problems waren die Aufsätze von Kummer (Liouville, Journal de Mathématiques pures et appliquées, Bd. XII u. XIV, Crelle's Journal Bd. 35, und Abhandlungen der Berliner Academie Jahr 1856). Grundlegend für die Methode der Behandlung ist überall die „Theorie der algebraischen Zahlen" meines hochverehrten Lehrers, Geheimrat Dr. K. Hensel, Professor an der Universität Marburg (dieses Werk wird in der Arbeit zur Abkürzung durch H. bezeichnet) und seine „Zahlentheorie". Die vorliegende Arbeit behandelt in Abschnitt I die Lagrange'schen Resolventen der Kreisteilungsgleichung vom Primzahlgrade, und man wird sehen, wie da auf Grund der Hensel'schen Theorie der algebraischen Zahlen die Primteilerzerlegung der Resolvente auf eine sehr viel einfachere und natürlichere Weise durchgeführt werden kann als es Kummer möglich war. In Abschnitt II und III leistet die Hensel'sche Theorie der algebraischen Zahlen die Primteilerzerlegung der Lagrange'schen Resolventen, welche diejenigen Kreisteilungsgleichungen auflösen, deren Grad bezw. eine Potenz einer ungeraden Primzahl, bezw. eine Potenz von 2 ist. Abschnitt IV behandelt die Resolvente für den allgemeinsten Fall, dass der Grad der Kreisteilungsgleichung eine beliebige zusammengesetzte Zahl ist. — Eine anderweitige Behandlung der in Abschnitt II—IV bearbeiteten Aufgaben liegt bis jetzt nicht vor.

Abschnitt I.

Die Resolvente der Gleichung $x^p - 1 = 0$.

Sei p eine ungerade Primzahl, ε eine primitive Wurzel der Gleichung

$$x^{p-1} - 1 = 0,$$

g eine primitive Congruenzwurzel modulo p. (Der allgemeinste von Kummer behandelte Fall ist der, dass man ε als nicht primitive Wurzel jener Gleichung annimmt.) Ist dann ω eine primitive Wurzel der Gleichung

$$x^p - 1 = 0,$$

so hat die Gleichung die folgende Lagrange'sche Resolvente

$$(\varepsilon, \omega) = \omega + \varepsilon \cdot \omega^g + \varepsilon^2 \cdot \omega^{g^2} + \ldots + \varepsilon^{p-2} \cdot \omega^{g^{p-2}}.$$

Wir gehen von der bekannten, später allgemein bewiesenen Tatsache aus, dass diese Resolvente nur solche Primfaktoren enthält, welche zugleich in p enthalten sind. — Wir betrachten zunächst den Körper $K(p, \omega)$, dann den Körper $K(p, \varepsilon)$, sodann den aus beiden zusammengesetzten Körper $K(p, \varepsilon, \omega)$, um dann die Primteilerzerlegung der Resolvente zu leisten.

§ 1. Der Körper $K(p, \omega)$.

Die Gleichung für die primitiven Wurzeln der Gleichung $x^p - 1 = 0 \ (p)$ lautet

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = (x - \omega)(x - \omega^2) \ldots (x - \omega^{p-1}) \ (p).$$

Setzt man darin $x = 1$, so kommt

$$p = (1 - \omega)(1 - \omega^2) \ldots (1 - \omega^{p-1}) \ (p).$$

Wir wollen nun allgemein $(1-\omega^i)$ durch π_i bezeichnen, π_1 auch durch π. Es ist p Verzweigungszahl $(p-1)$ter Ordnung des Körpers $K(p, \omega)$ und π wirklich Primzahl darin (siehe H. S. 138). Der Körper ist ein Galois'scher Körper und von der $(p-1)$ten Ordnung. Die π_i unterscheiden sich nur um Einheiten, es ist $p = E \cdot \pi^{p-1}$, wo E eine Haupteinheit ist; die ω^i sind Haupteinheiten. Die Zahlen $1, \omega, \omega^2, \ldots, \omega^{p-2}$ bilden ein absolutes Fundamentalsystem, ebenso das System

$$1, \pi, \pi^2, \ldots, \pi^{p-2},$$

welches aus jenem durch eine Substitution hervorgeht, deren Determinante 1 ist. Die Körperdiskriminante ist

$$\begin{vmatrix} 1 & \pi & \pi^2 & \ldots & \pi^{p-2} \\ 1 & \pi_2 & \pi_2^2 & \ldots & \pi_2^{p-2} \\ \cdot & & & & \\ \cdot & \cdot & & & \\ \cdot & & & & \\ \cdot & & & & \\ 1 & \pi_{p-1} & \pi_{p-1}^2 & \ldots & \pi_{p-1}^{p-2} \end{vmatrix}^2 \sim p^{p-2}.$$

§ 2. Der Körper $K(p, \varepsilon)$.

Es bezeichne ε_1 eine primitive Wurzel der Gleichung

$$x^{p-1} - 1 = 0 \quad (p),$$

und zwar diejenige, deren Anfangsziffer in der p-adischen Entwicklung g sei, wenn g die schon oben eingeführte Congruenzwurzel modulo p bezeichnet. Es sind alle primitiven Wurzeln der obigen Gleichung gegeben in der Reihe

$$\varepsilon_1^{a_1} = \varepsilon_1, \ \varepsilon_1^{a_2} = \varepsilon_2, \ \varepsilon_1^{a_3} = \varepsilon_3, \ \ldots, \ \varepsilon_1^{a_{\varphi(p-1)}} = \varepsilon_{\varphi(p-1)},$$

wo die a_i ein System aller Zahlen bedeuten, welche kleiner

als $(p-1)$ und relativ prim zu $(p-1)$ sind. Die Gleichung für diese primitiven $\varepsilon_1^{a_i}$,

$$\Phi(x) = (x - \varepsilon_1)(x - \varepsilon_1^{a_2}) \ldots\ldots (x - \varepsilon_1^{a\varphi(p-1)}) = 0$$

ist im Körper $K(1)$ irreducibel, im Körper $K(p)$ zerfällt sie in Linearfaktoren. Wir ordnen demnach (H. Kap. 7, § 3) jeder Wurzel $\varepsilon_1^{a_i} = \varepsilon_i$ einen Primteiler $\mathfrak{p}_i$ von p zu. Die ε_i sind rationale p-adische Zahlen, p also Primzahl für jeden Bereich $K(p, \varepsilon_i)$. Es ist

$$p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_{\varphi(p-1)}.$$

Für den Körper $K(p, \varepsilon)$, betrachtet inbezug auf jeden Primteiler $\mathfrak{p}_i$, bedeutet die Zahl 1 ein Fundamentalsystem. Wir können nun $\varphi(p-1)$ Zahlen $\chi_1(\varepsilon)$, $\chi_2(\varepsilon)$, ..., $\chi_{\varphi(p-1)}(\varepsilon)$ so wählen, dass jedesmal $\chi_i(\varepsilon_i) = 1$ wird, aber immer $\chi_i(\varepsilon_k) = 0$ für jedes $k \neq i$. Dann ist die Körperdiskriminante von $K(p, \varepsilon)$ das Quadrat der folgenden $\varphi(p-1)$-gliedrigen Determinante

$$\begin{vmatrix} 1\,0\,0\,\ldots\,0 \\ 0\,1\,0\,\ldots\,0 \\ \cdot \\ \cdot \\ \cdot \\ 0\,0\,0\,\ldots\,1 \end{vmatrix},$$

und ihr Wert ist 1.

§ 3. Der Körper $K(p, \varepsilon, \omega)$.

Wir setzen nun die Körper $K(p, \omega)$ und $K(p, \varepsilon)$ nach dem Hensel'schen Verfahren zusammen. (Hensel, über Gattungen, welche durch Composition aus zwei anderen Gattungen entstehen. Crelle's Journal Band 105). Wir sahen, dass die Discriminante des Körpers $K(p, \varepsilon)$ überhaupt p nicht enthält. Wir bekommen dann ein Fundamentalsystem für den Körper $K(p, \omega, \varepsilon)$, wenn wir alle Elemente des Fundamentalsystems

des einen Körpers mit allen Elementen des Fundamentalsystems des anderen Körpers multiplicieren. Das Fundamentalsystem für den Körper $K(p, \omega, \varepsilon)$ ist dann folgendes System von $(p-1)\cdot\varphi(p-1)$ Elementen

$$1,\ \pi,\ \pi^2,\ \ldots,\ \pi^{p-2},\ 0,\ 0,\ 0,\ \ldots,\ 0,$$

und die Körperdiscriminante ist das Quadrat folgender Determinante von $(p-1)\cdot\varphi(p-1)$ Gliedern

$$\begin{array}{|cccccccccccc|}
1\,\pi & \pi^2 & \ldots\pi^{p-2} & 0\,0 & 0 & \ldots 0 & & & \ldots\ldots\ldots & & & 0 \\
1\,\pi_2 & \pi_2^2 & \ldots\pi_2^{p-2} & . & & & & & & & & . \\
\vdots & & & . & & & & & & & & . \\
1\,\pi_{p-1} & \pi_{p-1}^2 & \ldots\pi_{p-1}^{p-2} & . & & & & & & & & . \\
0\,0 & 0 & \ldots 0 & 1\,\pi & \pi^2 & \ldots\pi^{p-2} & & & & & & . \\
0\ldots\ldots\ldots & & 0 & 1\,\pi_2 & \pi_2^2 & \ldots\pi_2^{p-2} & & & & & & . \\
\vdots & & & \vdots & & & & & & & & . \\
0 & & & 1\,\pi_{p-1} & \pi_{p-1}^2 & \ldots\pi_{p-1}^{p-2} & & & & & & . \\
. & & & & & & \ddots & & & & & . \\
. & & & & & & & 1\,\pi & \pi^2 & \ldots & \pi^{p-2} & \\
. & & & & & & & 1\,\pi_2 & \pi_2^2 & \ldots & \pi_2^{p-2} & \\
. & & & & & & & \vdots & & & & \\
0\ldots\ldots\ldots & & & & & & & 1\,\pi_{p-1} & \pi_{p-1}^2 & \ldots & \pi_{p-1}^{p-2} &
\end{array}.$$

Der Körper $K(\varepsilon, \omega)$ ist der Körper der $p\cdot(p-1)$ ten Einheitswurzeln $\varepsilon\cdot\omega$, er ist definiert durch die Gleichung

$$x^{p(p-1)} - 1 = 0.$$

Die Gleichung vom $(p-1)\cdot\varphi(p-1)$ ten Grade für die primitiven Wurzeln dieser Gleichung ist im Körper $K(1)$ irreducibel; im Körper $K(p)$ aber genügt jedes System

$$\varepsilon_1^{a_h}\cdot\omega,\ \varepsilon_1^{a_h}\cdot\omega^2,\ \varepsilon_1^{a_h}\cdot\omega^3,\ \ldots,\ \varepsilon_1^{a_h}\cdot\omega^{p-1}$$

für sich einer irreduciblen Gleichung $(p-1)$ ten Grades. Jedem solchen Zyklus ist eine Stelle $\mathfrak{p}_h$ zugeordnet. Zerfällt

man eine solche irreducible Gleichung weiter in ihre Linearfaktoren, so zerfällt der dieser Gleichung zugeordnete Primteiler $\mathfrak{p}_h$ weiter und zwar folgendermassen:

$$\mathfrak{p}_h \sim \mathfrak{P}_h^{p-1}.$$

Primzahl an jeder solchen Stelle $\mathfrak{P}_h$ ist π, und alle Zahlen des Körpers $K(p, \varepsilon, \omega)$ lassen sich darstellen in der Form

$$\alpha = \pi^{\varrho}(a_0 + a_1\pi + a_2\pi^2 + \ldots)$$

wo die a_i modulo p reducierte ganze Zahlen sind. Wollen wir nun eine algebraische Zahl $\chi(\varepsilon)$ inbezug auf ihre Teilbarkeit durch einen Primteiler $\mathfrak{P}_h$ untersuchen, so entwickeln wir $\chi(\varepsilon_1^{a_h})$ nach steigenden Potenzen von π. Ist die sich dann ergebende Ordnungszahl etwa s, so ist $\chi(\varepsilon)$ genau durch $\mathfrak{P}_h^s$ teilbar.

§ 4. (ε, ω) ist genau durch $\mathfrak{P}_1^{p-2}$ teilbar.

Nach diesem Verfahren wollen wir nun die Teilbarkeit der Zahl (ε, ω) inbezug auf die Primteiler $\mathfrak{P}_i$ feststellen. Wir haben also alle Ausdrücke $(\varepsilon_1^{a_i}, \omega)$ auf ihre Teilbarkeit durch π hin zu untersuchen. Wir untersuchen zunächst (ε_1, ω). Es ist

$$\omega = 1, \quad -1 \quad 0 \quad 0 \ldots \quad (\pi)$$

die π-adische Darstellung von ω, also

$$\omega^{g^k} = 1, \quad -\binom{g^k}{1} \quad \binom{g^k}{2} \quad -\binom{g^k}{3} \quad \binom{g^k}{4} \ldots \quad (\pi),$$

wo allgemein für $g^k < l$ $\binom{g^k}{l} = 0$ ist. Setzen wir das in $(\varepsilon_1, \omega) = \sum_{k=0}^{p-2} \varepsilon_1^k \cdot \omega^{g^k}$ ein, so bekommen wir

$$(\varepsilon_1, \omega) = \sum_{k=0}^{p-2} \varepsilon_1^k, \quad -\sum_{k=0}^{p-2} \varepsilon_1^k \binom{g^k}{1} \quad \sum \varepsilon_1^k \binom{g^k}{2} \quad -\sum \varepsilon_1^k \binom{g^k}{3} \ldots \quad (\pi).$$

Wir betrachten diese π-adische Zahl jetzt modulo p, also modulo π^{p-1}; das wird genügen, weil wir sehen werden, dass (ε_1, ω) durch eine geringere Potenz von π teilbar ist. Um dann diese Potenz von π festzustellen, brauchen wir nur zu untersuchen, welche von den Ziffern als erste nicht mehr durch p teilbar ist. Da nun

$$\varepsilon_1 \equiv g \mod \pi^{p-1}$$

ist, ersetzen wir oben überall g durch ε_1. Dann bekommen wir

$$(\varepsilon_1, \omega) \equiv \sum_{k=0}^{p-2} \varepsilon_1^k, \quad -\Sigma\varepsilon_1^{2k} \quad \Sigma\varepsilon_1^k\binom{\varepsilon_1^k}{2} \quad -\Sigma\varepsilon_1^k\binom{\varepsilon_1^k}{3}\ldots \bmod \pi^{p-1}.$$

Die allgemeine $h$te Ziffer dieser Zahl ist

$$\sum_{k=0}^{p-2} \varepsilon_1^k\binom{\varepsilon_1^k}{h} = \frac{1}{h!}\cdot\left\{\sum_{k=0}^{p-2}\varepsilon_1^{k(h+1)} + z_0^{(h)}\cdot\Sigma\varepsilon_1^{k\cdot h} + z_1^{(h)}\cdot\Sigma\varepsilon_1^{k(h-1)} + \ldots\right.$$

$$\left. + z_{h-1}^{(h)}\,\Sigma\varepsilon_1^k\right\},$$

wo die $z_i^{(h)}$ rationale Zahlen sind, und sogar modulo p ganze, solange $h<p$ ist. Nun ist

$$\sum_{k=0}^{p-2}\varepsilon_1^{k\cdot i} = \frac{\varepsilon_1^{(p-1)i} - 1}{\varepsilon_1^i - 1}$$

und also

$$\sum_{k=0}^{p-2}\varepsilon_1^{ki} = 0 \quad (p)$$

solange $i<p-1$ ist. Erst diejenige Summe $\sum_{k=0}^{p-2}\varepsilon_1^k\binom{\varepsilon_1^k}{h}$ also, in welcher die erste Summe, $\sum_{k=0}^{p-2}\varepsilon_1^{k(h+1)}$, nicht mehr null ist, also

$$h+1 = p-1,$$
$$h = p-2$$

ist, ist als erste nicht mehr gleich null. Das ist also die Ziffer

$$\sum_{k=0}^{p-2} \varepsilon_1^k \binom{\varepsilon_1^k}{p-2}.$$

Für diese ergibt sich

$$\sum_{k=0}^{p-2} \varepsilon_1^k \binom{\varepsilon_1^k}{p-2} = \frac{1}{(p-2)!} \cdot \Sigma\, \varepsilon_1^{k(p-1)} = -1, \ \ldots \quad (p),$$

und daraus folgt schliesslich

$$(\varepsilon_1,\ \omega) = \pi^{p-2} \cdot E,$$

wo E eine π-adische Haupteinheit bedeutet. Also ist (ε, ω) durch

$$\mathfrak{P}_1^{p-2}$$

genau teilbar, oder: es ist $(\varepsilon, \omega)^{p-1}$ durch $\mathfrak{p}_1^{p-2}$ teilbar.

§ 5. Das Resultat: $(\varepsilon, \omega) = \prod_{h=1}^{\varphi(p-1)} \mathfrak{P}_h^{p-1-a_h}$.

Allgemein ergibt sich für $(\varepsilon_1^{a_h}, \omega)$ in wörtlich derselben Weise:

$$(\varepsilon_1^{a_h}, \omega) = \sum_{k=0}^{p-2} \varepsilon_1^{ka_h}, \quad -\Sigma\, \varepsilon_1^{k(a_h+1)} \quad \Sigma\, \varepsilon_1^{ka_h} \binom{\varepsilon_1^k}{2} \quad -\Sigma\, \varepsilon_1^{ka_h} \binom{\varepsilon_1^k}{3} \ldots$$

$$\bmod \pi^{p-1},$$

und genau ebenso folgt, dass darin

$$\Sigma\, \varepsilon_1^{ka_h} \binom{\varepsilon_1^k}{p-1-a_h}$$

die erste von null verschiedene Ziffer ist.
Man bekommt

$$(\varepsilon_1^{a_h}, \omega) = \frac{(-1)^{a_h+1}}{(p-1-a_h)!} \cdot \pi^{p-1-a_h} + \ldots = a_h! \cdot \pi^{p-1-a_h} + \ldots \quad (\pi)$$

wobei $a_h!$ eine Einheit für den Bereich von π ist. Es folgt, dass (ε, ω) genau durch

$$\mathfrak{P}_h^{p-1-a_h}$$

teilbar ist, oder $(\varepsilon, \omega)^{p-1}$ durch $\mathfrak{p}_h^{p-1-a_h}$.

Fassen wir nun das Gefundene zusammen, so erhalten wir folgende Resultate

$$(\varepsilon,\ \omega) = \prod_{h=1}^{\varphi(p-1)} \mathfrak{P}_h^{p-1-a_h},$$

oder

$$(\varepsilon,\ \omega)^{p-1} = \prod_{h=1}^{\varphi(p-1)} \mathfrak{p}_h^{p-1-a_h}.$$

§ 6. Die von Kummer behandelte Resolvente.

Man kann mit leichter Mühe die gefundenen Resultate auf den Fall ausdehnen, dass jetzt ε primitive Wurzel der Gleichung

$$x^n - 1 = 0$$

ist, wo $n = \dfrac{p-1}{m}$ eine beliebig zusammengesetzte oder eine Primzahl ist, welche als Teiler in $(p-1)$ enthalten ist. Die so definierte Resolvente (ε, ω) ist die allgemeinste von Kummer in ihre Primteiler zerlegte Resolvente. — Man sieht sehr leicht, — wenn man wörtlich dieselben Rechnungen durchführt wie vorhin, — dass man in den Resultaten nur $(p-1)$ durch n zu ersetzen hat, während die $\mathfrak{P}_i$, die $\mathfrak{p}_i$ und die a_h die entsprechend abgeänderten Bedeutungen haben. Man findet

$$(\varepsilon,\ \omega) = \prod_{h=1}^{\varphi(n)} \mathfrak{P}_h^{n-a_h}$$

$$(\varepsilon,\ \omega)^n = \prod_{h=1}^{\varphi(n)} \mathfrak{p}_h^{n-a_h}.$$

Dem entsprechend ist

$$(\varepsilon^{-1},\ \omega)^n = (\varepsilon^{n-1},\ \omega)^n = \prod_{h=1}^{\varphi(n)} \mathfrak{p}_h^{a_h}.$$

Dieses letztere Resultat ist identisch mit dem von Kummer gefundenen allgemeinsten, wovon man sich durch Einführung der Kummer'schen Bezeichnungen leicht überzeugen kann.

Abschnitt II.

Die Resolvente der Gleichung $x^{p^v} - 1 = 0$.

Wir betrachten nun die Lagrange'sche Resolvente der Kreisteilungsgleichung

$$x^{p^v} - 1 = 0,$$

wo p wieder eine ungerade Primzahl ist, und nun $v > 1$, sonst aber eine beliebige ganze Zahl. Sei ω eine primitive Wurzel der obigen Gleichung. — Wir wollen in folgendem immer abkürzend $\varphi(p^i)$ durch φ_i bezeichnen. Ist dann ε eine primitive Wurzel der Gleichung

$$x^{\varphi_v} - 1 = 0,$$

und g eine primitive Wurzel der Congruenz

$$x^{\varphi_v} - 1 \equiv 0 \bmod p^v,$$

dann lautet die zu betrachtende Lagrange'sche Resolvente

$$(\varepsilon, \omega) = \omega + \varepsilon \cdot \omega^g + \varepsilon^2 \cdot \omega^{g^2} + \varepsilon^3 \cdot \omega^{g^3} + \ldots + \varepsilon^{\varphi_v - 1} \cdot \omega^{g^{\varphi_v - 1}}.$$

Da die Resolvente eine ganze Zahl ist und ausserdem Teiler von p, wie wir später (s. § 10) zeigen werden, so kann sie nur solche Primfaktoren enthalten, die zugleich in p enthalten sind. — Wir betrachten nun wieder die Körper $K(p, \omega)$ und $K(p, \varepsilon)$, um dann wieder $K(p, \varepsilon, \omega)$ zusammenzusetzen.

§ 1. Der Körper $K(p, \omega)$.

Der Körper $K(p, \omega)$ ist definiert durch die Gleichung

$$x^{p^v} - 1 = 0 \quad (p).$$

Deren primitive Wurzeln sind definiert durch die Gleichung

$$\frac{x^{p^v} - 1}{x^{p^{v-1}} - 1} = x^{p^{v-1}(p-1)} + x^{p^{v-1}(p-2)} + \ldots + x^{p^{v-1}} + 1 = 0 \ (p).$$

Diese ist sowohl im Körper $K(1)$ wie auch im Körper $K(p)$ irreducibel. Ist ω eine primitive Wurzel und hat g die oben

angegebene Bedeutung, so sind

$$\omega,\ \omega^g,\ \omega^{g^2},\ \omega^{g^3},\ \ldots,\ \omega^{g^{\varphi_v-1}}$$

alle primitiven Wurzeln. Bezeichnen wir jedes $1-\omega^{g^{i-1}}$ durch π_i, speziell $1-\omega$ durch $\pi_1=\pi$, so erhält man, wenn man in der Gleichung für die primitiven ω $x=1$ einsetzt,

$$p=\pi_1\cdot\pi_2\cdot\ldots\cdot\pi_{\varphi_v}.$$

Die π_i sind äquivalent, d. h. sie unterscheiden sich nur um Einheiten; also ist

$$p=E\cdot\pi^{\varphi_v},$$

wo E eine Einheit ist. π ist wirklich Primzahl im Bereiche $K(p,\omega)$ (siehe H, S. 138) und p Verzweigungszahl φ_v ter Ordnung darin. Der Körper ist ein Galois'scher Körper von φ_v ter Ordnung. Die ω^i sind Haupteinheiten. Die Zahlen

$$1,\ \pi,\ \pi^2,\ \ldots,\ \pi^{\varphi_v-1}$$

bilden ein absolutes Fundamentalsystem für den Körper $K(p,\omega)$, die Körperdiskriminante ist

$$\begin{vmatrix} 1 & \pi & \pi^2 & \ldots & \pi^{\varphi_v-1} \\ 1 & \pi_2 & \pi_2^2 & \ldots & \pi_2^{\varphi_v-1} \\ \vdots & & & & \\ 1 & \pi_{\varphi_v} & \pi_{\varphi_v}^2 & \ldots & \pi_{\varphi_v}^{\varphi_v-1} \end{vmatrix}^2,$$

deren Wert $p^{p^{v-1}(pv-v-1)}$ ist.

§ 2. Der Körper $K(p,\varepsilon)$

Der Körper $K(p,\varepsilon)$ ist definiert durch die Gleichung

$$x^{\varphi_v}-1=0\quad(p).$$

Sei ε_1 eine primitive Wurzel dieser Gleichung, die übrigen seien wieder bezeichnet durch $\varepsilon_1^{a_i}$. Ihre Anzahl ist $p^{v-2}(p-1)\cdot\varphi(p-1)$,

ihre Gleichung also von diesem Grade. Diese ist im Körper $K(1)$ irreducibel, im Bereiche $K(p)$ aber nicht. Sind

$$\alpha_1,\ \alpha_2,\ \alpha_3,\ \ldots,\ \alpha_{\varphi(p-1)}$$

alle primitiven Wurzeln der Gleichung

$$x^{p-1} - 1 = 0 \quad (p),$$

und

$$\beta_1,\ \beta_2,\ \beta_3,\ \ldots.,\ \beta_{\varphi_{v-1}}$$

alle primitiven Wurzeln der Gleichung

$$x^{p^{v-1}} - 1 = 0 \quad (p),$$

so sind alle primitiven Wurzeln ε_i gegeben in den Zyklen

$$\alpha_i\beta_1,\ \alpha_i\beta_2,\ \alpha_i\beta_3,\ \ldots,\ \alpha_i\beta_{\varphi_{v-1}},$$

für $i = 1, 2, 3, \ldots, \varphi(p-1)$. Jeder dieser $\varphi(p-1)$ Zyklen genügt für sich einer im Körper $K(p)$ irreducibeln Gleichung. Will man alle primitiven $\varepsilon_i = (\alpha_h\beta_k)$ als Potenzen eines einzigen, $\varepsilon_1 = \alpha_1 \cdot \beta_1$, darstellen, so sind es alle diejenigen Potenzen von ε_1, für deren Exponent

$$(a,\ \varphi(p^2)) = 1$$

ist. Von diesen $\varepsilon_1^a = (\alpha_1 \cdot \beta_1)^a$ gehören alle diejenigen zu einem Zyklus zusammen, deren Exponenten modulo $(p-1)$ congruent sind, weil α^a für modulo $(p-1)$ congruente Werte a denselben Wert ergibt.

Sind

$$a_1,\ a_2,\ a_3,\ \ldots,\ a_{\varphi(p-1)}$$

ein System von $\varphi(p-1)$ verschiedenen Zahlen, welche alle kleiner als $(p-1)$ und relativ prim zu $(p-1)$ sind, so genügt also jedes der hierzu gehörigen $\varepsilon_1^{a_i}$ einer andern der $\varphi(p-1)$ in $K(p)$ irreducibeln Gleichungen. Wir bezeichnen daher den der Gleichung, welcher $\varepsilon_1^{a_i}$ genügt, zugeordneten Primteiler durch $\mathfrak{p}_i$. Diese Primteiler sind dann

$$\mathfrak{p}_1,\ \mathfrak{p}_2,\ \mathfrak{p}_3,\ \ldots,\ \mathfrak{p}_{\varphi(p-1)}.$$

Da die α_i rationale p-adische Zahlen sind, so ist die Primzahl $\varkappa = 1 - \beta \sim p^{\frac{1}{\varphi_{v-1}}}$ des Körpers $K(p, \beta)$ auch Primzahl im Bereiche $K(p, \varepsilon)$. Dabei folgt aus der Beziehung $\beta^p = \omega$ leicht, dass $\varkappa \sim \pi^p$ ist. Andrerseits ist

$$\varkappa \sim \pi^p \sim \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_{\varphi(p-1)}.$$

Fundamentalsystem und Körperdiskriminante des Körpers $K(p, \varepsilon)$ findet man wörtlich nach der in Abschnitt I angegebenen Weise, indem man die Körper $K(\alpha)$ und $K(\beta)$ zusammensetzt. Wir erhalten dann als Fundamentalsystem des Körpers $K(p, \varepsilon)$ folgendes System von $\varphi(p^{v-1}) \cdot \varphi(p-1)$ Elementen:

$$1,\ \varkappa,\ \varkappa^2,\ \varkappa^3,\ \ldots,\ \varkappa^{\varphi_{v-1}-1},\ 0,\ 0,\ 0,\ \ldots,\ 0,$$

und Körperdiskriminante ist das Quadrat folgender Determinante von $\varphi(p^{v-1})\,\varphi(p-1)$ Gliedern

$$\begin{array}{cccccccccc}
1 & \varkappa & \varkappa^2 & \ldots \varkappa^{\varphi_{v-1}-1} & 0 & 0 & 0 & \ldots 0 & \ldots\ldots\ldots & 0 \\
1 & \varkappa_2 & \varkappa_2^2 & \ldots \varkappa_2^{\varphi_{v-1}-1} & 0 & & & & & \vdots \\
\vdots & & & & \vdots & & & & & \\
1 & \varkappa_{\varphi_{v-1}} & \varkappa_{\varphi_{v-1}}^2 & \ldots \varkappa_{\varphi_{v-1}}^{\varphi_{v-1}-1} & 0 & & & & & \\
0 & 0 & 0 & \ldots 0 & 1 & \varkappa & \varkappa^2 & \ldots \varkappa^{\varphi_{v-1}-1} & & \\
0 & 0 & 0 & \ldots 0 & 1 & \varkappa_2 & \varkappa_2^2 & \ldots \varkappa_2^{\varphi_{v-1}-1} & & \\
\vdots & & & & \vdots & & & & & \\
0 & & & & 1 & \varkappa_{\varphi_{v-1}} & \varkappa_{\varphi_{v-1}}^2 & \ldots \varkappa_{\varphi_{v-1}}^{\varphi_{v-1}-1} & & \\
 & & & & & & & & 1\ \varkappa & \varkappa^2 \quad \ldots \varkappa^{\varphi_{v-1}-1} \\
 & & & & & & & & 1\ \varkappa_2 & \varkappa_2^2 \quad \ldots \varkappa_2^{\varphi_{v-1}-1} \\
0 & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & & & & 1\ \varkappa_{\varphi_{v-1}} & \varkappa_{\varphi_{v-1}}^2 \quad \ldots \varkappa_{\varphi_{v-1}}^{\varphi_{v-1}-1}
\end{array}.$$

§ 3. Der Körper $K(p, \varepsilon, \omega)$.

Wir wollen nun den Körper $K(p, \varepsilon, \omega)$ bilden. Nun war $\varepsilon = \alpha \cdot \beta$ und $K(\beta)$ ein Unterkörper von $K(\omega)$. Also ist

$$K(p, \varepsilon, \omega) = K(p, \alpha, \omega),$$

und wir brauchen nur $K(p, \alpha)$ und $K(p, \omega)$ zusammenzusetzen. Das macht man nun auf wörtlich dieselbe Weise wie in § 2 die Zusammensetzung von $K(\alpha)$ und $K(\beta)$, nur dass jetzt der Exponent von p um 1 höher, nämlich v ist. Wir bekommen so ein Fundamentalsystem des Körpers $K(p, \alpha, \omega)$ in folgendem System von $\varphi(p^v) \cdot \varphi(p-1)$ Elementen

$$1,\ \pi,\ \pi^2,\ \pi^3,\ \ldots,\ \pi^{\varphi_v - 1},\ 0,\ 0,\ 0,\ \ldots,\ 0,$$

und die Körperdiskriminante ist das Quadrat folgender Determinante von $\varphi(p^v) \cdot \varphi(p-1)$ Gliedern:

$$\begin{vmatrix}
1 & \pi & \pi^2 & \ldots & \pi^{\varphi_v - 1} & 0 & & & & \\
1 & \pi_2 & \pi_2^2 & \ldots & \pi_2^{\varphi_v - 1} & 0 & & & & \\
\vdots & & & & & \vdots & & & & \\
1 & \pi_{\varphi_v} & \pi_{\varphi_v}^2 & \ldots & \pi_{\varphi_v}^{\varphi_v - 1} & 0 & & & & \\
0 & 0 & 0 & \ldots & 0 & 1 & \pi & \pi^2 & \ldots & \pi^{\varphi_v - 1} \\
\vdots & & & & & 1 & \pi_2 & \pi_2^2 & \ldots & \pi_2^{\varphi_v - 1} \\
 & & & & & \vdots & & & & \\
 & & & & & 1 & \pi_{\varphi_v} & \pi_{\varphi_v}^2 & \ldots & \pi_{\varphi_v}^{\varphi_v - 1} \\
 & & & & & & & & & \\
 & & & & & & & & 1 \ \pi & \pi^2 \ \ldots \ \pi^{\varphi_v - 1} \\
 & & & & & & & & 1 \ \pi_2 & \pi_2^2 \ \ldots \ \pi_2^{\varphi_v - 1} \\
 & & & & & & & & \vdots & \\
0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & 1 \ \pi_{\varphi_v} & \pi_{\varphi_v}^2 \ \ldots \ \pi_{\varphi_v}^{\varphi_v - 1}
\end{vmatrix}.$$

Die den Körper constituierende Gleichung ist

$$x^{\varphi_{v+1}} - 1 = 0 \ (p),$$

oder die daraus leicht zu erhaltende Gleichung für die primitiven $p^v(p-1)$ten Einheitswurzeln. Letztere ist aber

im Körper $K(p)$ wieder weiter reducibel. Bezeichnen wir wieder die primitiven $(p-1)$ ten π-adischen Einheitswurzeln durch $\alpha_1^{a_i}$, wo die a_i die vorhin angegebene Bedeutung haben, so genügen immer die Zahlen je eines Systems von primitiven $\varphi_{\nu+1}$ ten Einheitswurzeln der folgenden Art für sich einer in $K(p)$ irreducibeln Gleichung:

$$\alpha_1^{a_i}\omega,\ \alpha_1^{a_i}\omega^g,\ \alpha_1^{a_i}\omega^{g^2},\ \ldots,\ \alpha_1^{a_i}\omega^{g^{\varphi_\nu-1}}.$$

Einem jeden dieser $\varphi(p-1)$ Zyklen ist im Körper $K(p, \varepsilon)$ die seinem $\alpha_1^{a_i}$ entsprechende Stelle $\mathfrak{p}_i$ zugeordnet. Im Körper $K(p, \omega)$ zerfällt $\mathfrak{p}_i$ weiter und zwar entsprechend der Beziehung $\beta = \omega^p$ folgendermassen

$$\mathfrak{p}_i \sim \mathfrak{P}_i^p.$$

Da jedes α_i eine rationale p-adische Zahl ist, ist π Primzahl an jeder solchen Stelle $\mathfrak{P}_i$. Es ist

$$\pi \sim p^{\frac{1}{\varphi_\nu}} \sim \mathfrak{P}_1\mathfrak{P}_2\ldots\ldots\mathfrak{P}_{\varphi(p-1)}.$$

Der Zusammenhang zwischen den $\mathfrak{p}_i$ und den $\mathfrak{P}_i$ ist der, dass $\mathfrak{p}_i$ der der Wurzel $\varepsilon_i = \varepsilon_1^{a_i}$ im Körper $K(p, \varepsilon)$ zugeordnete Primteiler ist, $\mathfrak{P}_i$ der ihr im Körper $K(p, \omega)$ zugeordnete Primteiler.

Wollen wir nun eine Zahl $\chi(\varepsilon)$ inbezug auf ihre Teilbarkeit durch einen Primteiler $\mathfrak{P}_i$ untersuchen, so haben wir $\chi(\varepsilon_i)$ nach steigenden Potenzen von π zu entwickeln. Ist die sich ergebende Ordnungszahl etwa s, so ist $\chi(\varepsilon)$ genau durch $\mathfrak{P}_i^s$ teilbar.

§ 4. (ε_1, ω) als π-adische Zahl.

Nach diesem Verfahren werden wir jetzt die Zahlen (ε, ω) inbezug auf die Primteiler $\mathfrak{P}_i$ untersuchen, zunächst inbezug auf $\mathfrak{P}_1$.

Es sei

ω eine primitive Wurzel der Gleichung $x^{p^v} - 1 = 0 \quad (p)$

α_1 eine primitive Wurzel der Gleichung $x^{p-1} - 1 = 0 \quad (p)$

β_1 eine primitive Wurzel der Gleichung $x^{p^{v-1}} - 1 = 0 \quad (p)$

$\varepsilon_1 = \alpha_1 \cdot \beta_1$ eine primitive Wurzel der Gleichung $x^{\varphi_v} - 1 = 0 \quad (p)$

g eine primitive Wurzel der Congruenz $x^{\varphi_v} - 1 \equiv 0 \mod (p^v)$.

Die Entwicklung von (ε_1, ω) lautet

$$(\varepsilon_1, \omega) = \omega + \varepsilon_1 \cdot \omega^g + \varepsilon_1^2 \cdot \omega^{g^2} + \varepsilon_1^3 \cdot \omega^{g^3} + \ldots + \varepsilon_1^{\varphi-1} \omega^{g^{\varphi-1}},$$

wobei wir, wie in folgendem häufiger, $\varphi(p^v) = \varphi_v$ zur Abkürzung durch φ bezeichnen. Es folgt weiter

$$(\varepsilon_1, \omega) = \omega + \alpha_1 \beta_1 \omega^g + \alpha_1^2 \beta_1^2 \omega^{g^2} + \alpha_1^3 \beta_1^3 \omega^{g^3} + \ldots + \alpha_1^{\varphi-1} \beta_1^{\varphi-1} \omega^{g^{\varphi-1}}.$$

Da nun $\beta_1 = \omega^p$ ist, so ergibt sich

$$(\varepsilon_1, \omega) = \omega + \alpha_1 \omega^{p+g} + \alpha_1^2 \omega^{2p+g^2} + \alpha_1^3 \omega^{3p+g^3} + \ldots + \alpha_1^{\varphi-1} \omega^{(\varphi-1)p+g^{\varphi-1}}.$$

Nun ist

$$\omega = 1, \quad -1 \quad (\pi),$$

also

$$\omega^{pk+g^k} = 1, \quad -\binom{pk+g^k}{1} \quad \binom{pk+g^k}{2} \quad -\binom{pk+g^k}{3} \ldots \quad (\pi).$$

Setzt man das oben ein, so kommt

$$(\varepsilon_1, \omega) = \sum_{k=0}^{\varphi-1} \alpha_1^k \binom{pk+g^k}{0} - \pi \cdot \sum_{k=0}^{\varphi-1} \alpha_1^k \binom{pk+g^k}{1} + \pi^2 \cdot \sum \alpha_1^k \binom{pk+g^k}{2} - + \ldots.$$

§ 5. (ε_1, ω) als Summe von $(p-1)$ π-adische Zahlen:

$$(\varepsilon_1\ \omega) = \sum_{i=0}^{p-1} C_i\, \alpha_1^{k_i}.$$

Für k gibt es $(p-1)$ modulo $(p-1)$ incongruente Werte, diese seien, in irgend einer Reihenfolge, durch $k_1, k_2, \ldots, k_{p-1}$ bezeichnet. Alle möglichen verschiedenen Werte von α_1^k sind dann die Werte $\alpha_1^{k_1}, \alpha_1^{k_2}, \ldots, \alpha_1^{k_{p-1}}$. Wir ordnen jetzt den für (ε_1, ω) gewonnenen Ausdruck nach Potenzen von α. Wir bekommen

$$(\varepsilon_1\ \omega) = C_1\, \alpha_1^{k_1} + C_2\, \alpha_1^{k_2} + C_3\, \alpha_1^{k_3} + \ldots + C_{p-1}\, \alpha_1^{k_{p-1}},$$

worin allgemein

$$C_i = \sum_{h=0}^{\infty} (-\pi)^h \sum_{k \equiv k_i} \binom{pk + g^k}{h},$$

$$C_i = \sum_{k \equiv k_i} \binom{kp + g^k}{0} - \pi \sum_{k \equiv k_i} \binom{kp + g^k}{1} + \pi^2 \sum \binom{kp + g^k}{2} - + \ldots$$

ist, mit der Massgabe, dass jede Summe $\sum_{k \equiv k_i}$ über alle diejenigen p^{v-1} verschiedenen Werte k zwischen 0 und φ_v zu nehmen ist, für welche $k \equiv k_i \mod (p-1)$ ist.

Wir werden zeigen, dass von den C_i nur eines von null verschieden ist, während die übrigen verschwinden. Und zwar wird C_i stets dann verschwinden, wenn für das zu C_i gehörige k_i die Zahlen $pk+g^k$ mit den Zahlen g^k modulo p^v übereinstimmen. Man sieht zunächst: Die sämtlichen in einem bestimmten C_i vorkommenden Ausdrücke sind alles Zahlen der Form $np+g_{k_i}$, wenn g_{k_i} den kleinsten Rest von g^{k_i} modulo p bedeutet. Für jedes k_i gibt es p^{v-1} Zahlen $pk+g^k$. Sind diese nun alle von einander verschieden, so sind sie modulo p^v identisch mit allen Zahlen $np+g_k$, bezw. mit allen Zahlen g^k

für alle $k \equiv k_i$. Um nun unsern Beweis zu führen, werden wir nachweisen, dass für $p-2$ Werte k_i stets alle Werte $pk + g^k$ modulo p^v verschieden sind, für ein einziges nicht.

§ 6. Das nicht verschwindende C_1.

Wir werden das folgendermassen zeigen: Wir werden annehmen, dass zwei beliebige Werte $pk + g^k$ einander gleich seien, und werden daraus das zugehörige bestimmte k_i, welches wir durch k_1 bezeichnen wollen, berechnen. Sodann werden wir nachweisen, dass aus der Voraussetzung, dass irgend zwei andere beliebige Werte $pk + g^k$ einander gleich seien, sich mit Notwendigkeit immer dieses selbe bestimmte k_1 ergibt.

Es sei also etwa

$$pk + g^k \equiv p(k+z) + g^{k+z} \mod p^v,$$

wo z eine beliebige ganze Zahl sei. Damit die Congruenz zunächst mod p bestehen kann, muss z durch $(p-1)$ teilbar sein:

$$z = \zeta \cdot (p-1).$$

Setzen wir das ein, so ergibt sich daraus $k = k_1$ durch folgende Beziehung:

$$g^{k_1} \equiv -\frac{p(p-1)\zeta}{g^{(p-1)\zeta}-1} \mod p,$$

wo p den niedrigst möglichen Modul bezeichnet. Dieser genügt aber, weil k_1 nur modulo $(p-1)$ zu bestimmen ist. — Nun besteht für die primitive Congruenzwurzel g die Beziehung

$$g \equiv \bar{\alpha}\,(1 + p \cdot \gamma_0) \mod p^2$$

(siehe Hensel, Zahlentheorie I, S. 174) wobei $\bar{\alpha}$ eine primitive $(p-1)$te p-adische Einheitswurzel ist, und γ_0 eine durch p

nicht teilbare ganze Zahl. Es ergibt sich daher

$$g^{(p-1)\zeta} - 1 = (p-1) \cdot p \cdot \zeta \cdot \gamma_0 \cdot E \quad (p)$$

wo E eine p-adische Haupteinheit bedeutet. Setzt man das oben ein, so ergibt sich

$$g^{k_1} \equiv -\frac{1}{\gamma_0} \mod p.$$

Dieses Resultat ist von ζ unabhängig, man bekommt es also immer, ganz gleichgiltig wie man ζ wählt. Aus der Voraussetzung, dass irgend zwei Werte $pk + g^k$ einander gleich seien, bekommt man also immer dasselbe g^{k_1}. Damit ist bewiesen, dass es tatsächlich nur ein einziges $k \equiv k_1$ gibt, für welches die Werte $pk + g^k$ nicht alle von einander verschieden sind.

Wir wollen nun noch kurz zeigen, — was wir nachher gebrauchen werden, — dass die zu k_1 gehörigen Werte $pk + g^k$ sich so wiederholen, dass die Anzahl jedes vorkommenden Wertes durch p teilbar ist. Setzen wir nämlich einmal $\zeta = p^{\nu-2}$, so ergibt sich daraus wieder dasselbe g^{k_1} modulo p, wo nun aber p zugleich den höchstmöglichen Modul bedeutet. Das heisst: im Abstande $p^{\nu-2}(p-1)$ muss jeder zu k_1 gehörige Wert $pk + g^k$ wiederkehren, ebenso natürlich für $2 \cdot p^{\nu-2}(p-1)$ usw. Für

$$\sum_{k \equiv k_1} \binom{pk + g^k}{h} = \sum_{i=0}^{p^{\nu-1}-1} \binom{p(k_1 + i(p-1)) + g^{k_1 + i(p-1)}}{h}$$

ergibt sich also

$$\sum_{k \equiv k_1} \binom{pk + g^k}{h} = p \cdot \sum_{i=0}^{p^{\nu-2}-1} \binom{p(k_1 + i(p-1)) + g^{k_1 + i(p-1)}}{h},$$

und, wenn wir das Verschwinden der übrigen C_i bewiesen haben werden, erhalten wir darum, wovon wir in § 10 ausgehen werden,

$$(\varepsilon_1, \omega) = p \cdot \alpha_1^k \sum_{h=0}^{\infty} (-\pi)^h \cdot \sum_{i=0}^{p^{\nu-2}-1} \binom{p(k_1+i(p-1))+g^{k_1+i(p-1)}}{h}.$$

§ 7. Die verschwindenden C_i.

Wir fanden, dass es nur ein einziges $k = k_1$ gibt, für welches die Werte $pk + g^k$ nicht alle verschieden sind. Für alle andern k_i sind die zugehörigen Werte $pk + g^k$ alle von einander verschieden und stimmen also mit den Werten g^k überein, genommen über dieselben k. Es ist also in der Entwicklung $(\varepsilon_1, \omega) = \sum_{i=1}^{p-1} C_i \alpha_1^{k_i}$ für jedes $k_i \neq k_1$, also für $i = 2, 3, 4, \ldots, (p-1)$

$$C_i = \sum_{h=0}^{\infty} (-\pi)^h \sum_{k \equiv k_i} \binom{g^k}{h}.$$

Jede solche Zahl C_i verschwindet aber. Es ist nämlich folgender Ausdruck der obigen π-adischen Entwicklung gleich:

$$\sum_{k \equiv k_i} \omega^{g^k} = \omega^{g^{k_i}} + \omega^{g^{k_i+p-1}} + \omega^{g^{k_i+2(p-1)}} + \ldots + \omega^{g^{k_i+(p^{\nu-1}-1)(p-1)}}.$$

Das erkennt man, wenn man $\omega = 1 - \pi$ einsetzt. Der letztere Ausdruck verschwindet aber. Setzt man nämlich $\omega^{g^{k_i}} = \bar{\omega}$, wo $\bar{\omega}$ dann eine primitive p^{ν}te Einheitswurzel ist, so bekommt man für die obige Summe jetzt

$$\sum_{l=0}^{p^{\nu-1}-1} \bar{\omega}^{g^{l(p-1)}} = \bar{\omega} + \bar{\omega}^{g^{p-1}} + \bar{\omega}^{g^{2(p-1)}} + \ldots + \bar{\omega}^{g^{(p^{\nu-1}-1)(p-1)}}.$$

Nun sind alle Zahlen $g^{l(p-1)}$ modulo p^v identisch mit allen Zahlen $1+\lambda p$, denn in beiden Reihen ist jedes Glied von jedem andern verschieden, und die Anzahl der Glieder ist in beiden Reihen gleich gross. Man kann die obige Summe also schreiben

$$\bar{\omega} \cdot \sum_{\lambda=0}^{p^{v-1}-1} \bar{\omega}^{\lambda \cdot p},$$

und diese ist

$$\bar{\omega} \cdot \frac{1-\bar{\omega}^{p^v}}{1-\bar{\omega}^{p}} = 0.$$

Es verschwinden also alle C_i ausser dem einen C_1, und also ist jetzt

$$(\varepsilon_1, \omega) = C_1 \cdot \alpha_1^{k_1},$$

wo für C_1 der Ende § 6 gefundene Ausdruck zu setzen ist.

§ 8. Die Entwicklung von $(\varepsilon_1^{-1}, \omega)$.

Ebenso wie (ε, ω), wollen wir nun einmal den Ausdruck $(\varepsilon^{-1}, \omega)$ inbezug auf seine Teilbarkeit durch denselben Primteiler $\mathfrak{P}_1$ untersuchen. Wir betrachten also den Ausdruck

$$\begin{aligned}(\varepsilon_1^{-1}, \omega) &= \omega + \varepsilon_1^{-1}\omega^{g} + \varepsilon_1^{-2}\omega^{g^2} + \varepsilon_1^{-3}\omega^{g^3} + \ldots + \varepsilon_1^{-(\varphi-1)}\omega^{g^{\varphi-1}} \\ &= \omega + \alpha_1^{-1}\omega^{g-p} + \alpha_1^{-2}\omega^{g^2-2p} + \alpha_1^{-3}\omega^{g^3-3p} + \ldots \\ &\qquad + \alpha^{-(\varphi-1)} \cdot \omega^{g^{\varphi-1}-(\varphi-1)p} \\ &= \sum_{k=0}^{\varphi-1} \alpha_1^{-k}\omega^{g^k-pk},\end{aligned}$$

wofür wir lieber schreiben wollen

$$(\varepsilon_1^{-1}, \omega) = \sum_{k=0}^{\varphi-1} \alpha_1^{-k}(\omega^{-1})^{pk \cdot g^k}.$$

Wir entwickeln nun nach Potenzen von $(1 - \omega^{-1}) = \pi_{-1}$, in wörtlich derselben Weise, wie vorher (ε_1, ω) nach Potenzen von π. Dann ergibt sich

$$(\varepsilon_1^{-1}, \omega) = \sum_{h=0}^{\infty} (-\pi_{-1})^h \sum_{k=0}^{p-1} \alpha_1^{-k} \binom{pk - g^k}{h}.$$

Wir ordnen nach Potenzen von α^{-1} und bekommen für $(\varepsilon_1^{-1}, \omega)$, ganz entsprechend wie vorhin für (ε_1, ω) einen Ausdruck

$$(\varepsilon_1^{-1}, \omega) = C_{-1}\, \alpha_1^{-k-1} + C_{-2}\, \alpha_1^{-k-2} + \ldots + C_{-(p-1)}\, \alpha_1^{-k-(p-1)}.$$

Man zeigt auf wörtlich dieselbe Weise, dass von diesen C_{-i} wieder $(p-2)$ verschwinden, während ein einziges, welches durch C_{-1} bezeichnet sei, von null verschieden ist. Das zu letzterem gehörige k_{-1} ist ganz entsprechend wie damals definiert durch die Congruenz

$$pk - g^k \equiv p(k + \zeta(p-1)) - g^{k+\zeta(p-1)} \mod p^v,$$

und daraus ergibt sich

$$g^{k_{-1}} \equiv \frac{1}{\gamma_0} \mod p.$$

§ 9. (ε_1, ω) und $(\varepsilon_1^{-1}, \omega)$ enthalten dieselbe Potenz von π.

Wir erhalten für $g^{k_{-1}}$ also das Negative des Wertes, der sich für g^{k_1} ergab, es ist

$$-g^{k_{-1}} \equiv g^{k_1} \mod p.$$

Für k_1 wollen wir, wie schon früher, den kleinsten positiven unter den Werten $k_1 + i(p-1)$ annehmen. Dann ist k_{-1} durch die obige Congruenz zwar modulo $(p-1)$ bestimmt,

aber modulo γ_v noch nicht. Wir wollen jetzt k_{-1} so annehmen, dass die obige Congruenz auch modulo p^v besteht:

$$-g^{k_{-1}} \equiv g^{k_1} \mod p^v.$$

Daraus folgt

$$k_{-1} = k_1 + \frac{1}{2} \cdot \varphi(p^v).$$

Wir wollen nun zeigen, dass die sämtlichen Werte $pk - g^k$, die zu k_{-1} gehören, identisch sind mit den Werten $pk + g^k$, die zu k_1 gehören. Zunächst ist nämlich der zu k_{-1} gehörige Wert $pk_{-1} - g^{k_{-1}}$ identisch mit dem zu k_1 gehörigen Werte $p(k_1 + p^{v-2}(p-1)) + g^{k_1 + p^{v-2}(p-1)}$. Denn aus dieser Beziehung

$$pk_{-1} - g^{k_{-1}} \equiv p(k_1 + p^{v-2}(p-1)) + g^{k_1 + p^{v-2}(p-1)} \mod p^v$$

ergibt sich als notwendige und hinreichende Bedingung die Congruenz

$$g^{k_1} \equiv -\frac{1}{\gamma_0} \mod p,$$

und diese Congruenz ist als Definitionscongruenz für g^{k_1} jedenfalls richtig. Nehmen wir nun links den nächstfolgenden Wert aus C_{-1} und rechts den entsprechend nächstfolgenden Wert aus C_1, so ist die Beziehung

$$p(k_{-1} + p - 1) - g^{k_{-1}+p-1} \equiv p(k_1 + (p^{v-2} + 1)(p-1)) + g^{k_1 + (p^{v-2}+1)(p-1)} \mod p^v$$

wieder richtig, denn daraus ergibt sich wiederum als notwendige und hinreichende Bedingung

$$g^{k_1} \equiv -\frac{1}{\gamma_0} \mod p.$$

Genau ebenso stimmt jeder folgende Wert links mit jedem bezüglich folgenden Wert rechts überein. Es sind also die sämtlichen vorkommenden Werte $pk_1 + g^{k_1}$ identisch mit den sämtlichen vorkommenden Werten $pk_{-1} - g^{k_{-1}}$; d. h. für $\sum_{k \equiv k_{-1}} \binom{pk - g^k}{h}$ kann man schreiben $\sum_{k \equiv k_1} \binom{pk + g^k}{h}$.

Also: Ist

$$(\varepsilon_1, \omega) = \alpha_1^{k_1} \sum_{h=0}^{\infty} (-\pi)^h \cdot \sum_{k \equiv k_1} \binom{pk + g^k}{h},$$

so ist

$$(\varepsilon_1^{-1}, \omega) = \alpha_1^{-k_{-1}} \cdot \sum_{h=0} (-\pi_{-1})^h \sum_{k \equiv k_1} \binom{pk + g^k}{h}.$$

Das heisst: Abgesehen von der Einheit $\alpha_1^{k_1}$ bezw. $\alpha_1^{-k_{-1}}$, mit denen die beiden Ausdrücke beziehungsweise multipliciert sind, hat $(\varepsilon_1^{-1}, \omega)$, nach Potenzen von π_{-1} entwickelt, dieselben Ziffern wie (ε_1, ω), nach Potenzen von π entwickelt. Die π_i sind aber alle untereinander äquivalent, es enthält also $(\varepsilon_1^{-1}, \omega)$ dieselbe Potenz von π wie (ε_1, ω).

§ 10. (ε, ω) enthält die Potenz $\mathfrak{P}_1^{v \cdot \frac{\varphi_v}{2}}$.

Wir fanden Ende § 6 für (ε_1, ω)

$$(\varepsilon_1 \omega) = p \cdot \alpha_1^{k_1} \sum_{h=0}^{\infty} (-\pi)^h \sum_{i=0}^{p^{v-2}-1} \binom{p(k_1 + i(p-1)) + g^{k_1 + i(p-1)}}{h}.$$

Dafür kann man schreiben

$$(\varepsilon_1, \omega) = p \cdot \alpha_1^{k_1} \sum_{i=0}^{p^{v-2}-1} \omega^{p(k_1 + i(p-1)) + g^{k_1 + i(p-1)}}$$

wie man erkennt, wenn man $\omega = 1 - \pi$ einsetzt. Entsprechend ist

$$(\varepsilon_1^{-1}, \omega) = p \cdot \alpha_1^{-k_{-1}} \sum_{h=0}^{p^{\nu-2}-1} \omega^{-p(k_{-1} + h(p-1)) + g^{k_{-1}+h(p-1)}}$$

Daraus kann man nun die Potenz von π, die in dem Produkte $(\varepsilon_1, \omega)(\varepsilon_1^{-1}, \omega)$ enthalten ist, auf recht einfache Weise finden; sie ist $\pi^{\nu \cdot \varphi(p^\nu)}$. Etwas ähnliches beweist Weber, Algebra Bd. II, S. 69 ff., unser Beweis hier ist aber auf Grund der Reduktionen, die wir durch die π-adische Darstellung gewonnen haben, in wenigen Worten zu führen. Es ergibt sich nämlich durch Multiplikation unter Berücksichtigung der Beziehung $k_1 = k_{-1} + \frac{1}{2}\varphi_\nu$ jetzt

$$(\varepsilon_1^{-1}, \omega)(\varepsilon_1, \omega) = -p^2 \sum_{i=0}^{p^{\nu-2}-1} \sum_{h=0}^{p^{\nu-2}-1} \omega^{(i-h)(p-1)p + g^{k_1+h(p-1)}(1-g^{(i-h)(p-1)})}.$$

Ersetzen wir darin den Summationsindex $i - h$ durch i, so folgt

$$(\varepsilon_1^{-1}, \omega)(\varepsilon_1, \omega) = -p^2 \sum_{i=0}^{p^{\nu-2}-1} \omega^{i(p-1)p} \sum_{h=0}^{p^{\nu-2}-1} \omega^{g^{k_1+h(p-1)}(1-g^{i(p-1)})}.$$

Darin ist die Teilsumme inbezug auf h nur dann von null verschieden, wenn $g^{i(p-1)} - 1 \equiv 0 \bmod p^{\nu-1}$, wenn also i ein Vielfaches von $p^{\nu-2}$ ist. Das ist hier nur für den einzigen Wert $i = 0$ der Fall. Daraus ergibt sich sofort

$$(\varepsilon_1^{-1}, \omega)(\varepsilon_1, \omega) = -p^\nu.$$

Folglich ist

$$(\varepsilon_1\ \omega) \sim p^{\frac{\nu}{2}} \sim \pi^{\nu \cdot \frac{\varphi_\nu}{2}},$$

und also enthält (ε, ω) genau die Potenz

$$\mathfrak{P}^{v \cdot \frac{\varphi_v}{2}}.$$

§ 11. Das Resultat.

Will man die Teilbarkeit von (ε, ω) inbezug auf irgend einen anderen Primteiler $\mathfrak{P}_i$ untersuchen, so ist alles auf wörtlich dieselbe Weise zu machen wie für $\mathfrak{P}_1$. Man bildet $(\varepsilon_1^{a_i}, \omega)$, entwickelt nach Potenzen von π, zeigt, dass $(\varepsilon_1^{a_i}, \omega)$ dieselbe Potenz von π enthält wie $(\varepsilon_1^{-a_i}, \omega)$, und dann ergibt sich, dass (ε, ω) genau durch $\mathfrak{P}_i^{v \cdot \frac{\varphi_v}{2}}$ teilbar ist. Es ergibt sich also das Resultat

$$(\varepsilon, \omega) \sim \prod_{i=0}^{\varphi(p-1)} \mathfrak{P}_i^{v \cdot \frac{\varphi_v}{2}} = \pi^{v \cdot \frac{\varphi_v}{2}} = p^{\frac{v}{2}}.$$

Das Resultat ist hier ganz anders wie in Abschnitt I, für den Fall $v = 1$. Das kommt daher, wie man gewissermassen sagen könnte, dass der Exponent $v = 1$ zu klein ist. Man kann nämlich für $v = 1$ dieselbe π-adische Entwicklung der Resolvente hinschreiben wie für $v > 1$

$$(\varepsilon_1, \omega) = \sum_{h=0}^{\infty} (-\pi)^h \cdot \sum \alpha_1^k \binom{pk + g^k}{h},$$

nur kann man für $pk + g^k$ überall sofort schreiben g^k, weil da $\omega^p = 1$ ist. Für den Fall $v > 1$ ist aber gerade der Fall ausschlaggebend, dass man $pk + g^k$ nicht durch g^k ersetzen kann. — Wenn man es anders ausdrücken will, kann man auch sagen: Der Exponent φ_v, zu welchem ε hier gehört, hat mit dem Exponenten p^v von ω den grössten gemeinsamen Teiler p^{v-1}; in Abschnitt I sind die beiden entsprechenden Exponenten relativ prim zu einander.

Abschnitt III.

Die Resolvente der Gleichung $x^{2^\nu} - 1 = 0$.

Wir untersuchen nun die bisher ausgeschalteten Resolventen für die Kreisteilungsgleichungen der Form

$$x^{2^\nu} - 1 = 0.$$

Die Untersuchung verläuft im grossen und ganzen genau entsprechend den Untersuchungen in Abschnitt I und II. Es möge ω eine primitive Wurzel der obigen Gleichung bezeichnen. Die trivialen Fälle $\nu = 1$ und $\nu = 2$ seien ausgeschlossen, im übrigen sei ν eine beliebige positive ganze Zahl. Die Resolvente sieht hier etwas anders aus und zwar deshalb, weil es keine primitiven Wurzeln der Congruenz

$$x^{\varphi(2^\nu)} - 1 \equiv 0 \mod 2^\nu$$

gibt, sondern nur solche der Congruenz

$$x^{\frac{1}{2}\varphi(2^\nu)} - 1 \equiv 0 \mod 2^\nu,$$

und eine solche ist bekanntlich immer die Zahl 5. Infolge dessen wird auch ε als Wurzel der Gleichung

$$x^{\frac{1}{2}\varphi(2^\nu)} - 1 = 0$$

gewählt. Die Resolvente lautet dann

$$(-1, \varepsilon, \omega) = \omega - \omega^{-1} + \varepsilon(\omega^5 - \omega^{-5}) + \varepsilon^2(\omega^{5^2} - \omega^{-5^2}) + \ldots + \varepsilon^{\varphi'-1}(\omega^{5^{\varphi'-1}} - \omega^{-5^{\varphi'-1}}),$$

wobei zur Abkürzung $\frac{1}{2}\varphi(2^\nu) = 2^{\nu-2}$ durch φ' bezeichnet ist. Diese Resolvente ist eine ganze Zahl und gibt wieder, mit der Resolvente $(-1, \varepsilon^{-1}, \omega)$ multipliziert, eine Potenz von 2, und daraus folgt genau wie früher die Tatsache, dass die

Resolvente nur solche Primteiler enthalten kann, welche zugleich in 2 enthalten sind. — Wir betrachten nun wieder die Körper $K(2, \omega)$ und $K(2, \varepsilon)$, dann $K(2, \varepsilon, \omega)$.

§ 1. Der Körper $K(2, \omega)$.

Der Körper $K(2, \omega)$ ist definiert durch die Gleichung

$$x^{2^v} - 1 = 0 \quad (2),$$

eine Gleichung, die sowohl im Körper $K(1)$ wie im Körper der dyadischen Zahlen irreducibel ist. Ist ω eine primitive Wurzel, so ergeben sich alle in der Aufstellung

$$\omega,\ \omega^{-1},\ \omega^{5},\ \omega^{-5},\ \omega^{5^2},\ \omega^{-5^2},\ \ldots,\ \omega^{5^{\varphi'-1}},\ \omega^{-5^{\varphi'-1}}.$$

Bezeichnen wir allgemein $(1 - \omega^{\pm 5^{i-1}})$ durch $\pi_{\pm i}$, speciell auch π_1 durch π, so ist genau analog wie früher

$$2 = \pi_1 \cdot \pi_{-1} \cdot \pi_2 \cdot \pi_{-2} \ldots \pi_{\varphi'} \pi_{-\varphi'}.$$

Die $\pi_{\pm i}$ sind einander alle äquivalent. Wir nehmen daher eine unter ihnen, z. B. π, als Primzahl des Körpers an. Es ist

$$2 = E \cdot \pi^{2^{v-1}}$$

wo E eine Einheit bedeutet. π ist wirklich Primzahl in diesem Körper, 2 Verzweigungszahl 2^{v-1}ter Ordnung. Der Körper ist ein Galois'scher Körper und von der Ordnung 2^{v-1}.

Die Grössen $\omega^{\pm 5^i}$ sind Haupteinheiten. Ein Fundamentalsystem des Körpers wird gebildet durch die Zahlen

$$1,\ \pi,\ \pi^2,\ \pi^3,\ \ldots,\ \pi^{2^{v-1}-1}.$$

Die Körperdiskriminante ist gegeben in dem Determinantenquadrat

$$\begin{vmatrix} 1 & \pi & \pi^2 & \dots & \pi^{2^{v-1}-1} \\ 1 & \pi_{-1} & \pi_{-1}^2 & \dots & \pi_{-1}^{2^{v-1}-1} \\ 1 & \pi_2 & \pi_2^2 & \dots & \pi_2^{2^{v-1}-1} \\ 1 & \pi_{-2} & \pi_{-2}^2 & \dots & \pi_{-2}^{2^{v-1}-1} \\ & & & & \\ 1 & \pi_{-\varphi'} & \pi_{-\varphi'}^2 & \dots & \pi_{-\varphi'}^{2^{v-1}-1} \end{vmatrix}^2,$$

dessen Wert $2^{2^{v-1}(v-1)}$ ist.

§ 2. Der Körper $K(2, \varepsilon, \omega)$.

Wenden wir uns zur Betrachtung des Körpers $K(2, \varepsilon)$. Sei ε_1 eine primitive Wurzel der Gleichung

$$x^{2^{v-2}} - 1 = 0 \quad (2)$$

und zwar so gewählt, dass

$$\varepsilon_1^4 = \omega$$

ist. Es ist $K(2, \varepsilon)$ ein Unterkörper von $K(2, \omega)$. Die Gleichung für die primitiven Wurzeln ε_i, welche vom Grade 2^{v-3} ist, ist irreducibel, irreducibel auch im Bereiche $K(2)$. Die Primzahl des Körpers $K(2, \varepsilon)$ ist π^4. Da die Gleichung für die primitiven Wurzeln ε_i auch im Körper $K(2)$ irreducibel ist, ist allen diesen Wurzeln nur ein Primteiler zugeordnet, und dieser ist

$$\mathfrak{p} \sim \pi^4.$$

Da $K(\varepsilon_1)$ ein Unterkörper von $K(\omega)$ ist, so ist

$$K(2, \omega, \varepsilon_1) = K(2, \omega).$$

Der den Zahlen ε_i zugeordnete Primteiler p zerfällt hier weiter, gemäss der Beziehung

$$\mathfrak{p} \sim \mathfrak{P}^4,$$

wobei $\mathfrak{P} \sim \pi$ ist. Wir haben die vorgelegte Resolvente also nur auf ihre Teilbarkeit inbezug auf diesen einzigen Primteiler $\mathfrak{P}$ zu untersuchen.

§ 3. Die π-adische Entwicklung von $(-1, \varepsilon_1, \omega)$.

Sollen wir nun eine Zahl $\chi(\varepsilon)$ inbezug auf ihre Teilbarkeit durch $\mathfrak{P}$ untersuchen, so setzen wir für ε irgend eine primitive dyadische Wurzel ε_1^i ein, am einfachsten ε_1, und entwickeln nach Potenzen von π. Ist die sich ergebende Ordnungszahl etwa s, so ist $\chi(\varepsilon)$ genau durch $\mathfrak{P}^s$ teilbar. Nach diesem Verfahren wollen wir jetzt die Teilbarkeit von $(-1, \varepsilon, \omega)$ berechnen. Es ist

$$(-1, \varepsilon_1, \omega) = \omega - \omega^{-1} + \varepsilon_1 \omega^5 - \varepsilon_1 \omega^{-5} + \varepsilon_1^2 \omega^{5^2} - \varepsilon_1^2 \omega^{-5^2} + - \ldots + \varepsilon_1^{\varphi'-1} \omega^{5^{\varphi'-1}} - \varepsilon_1^{\varphi'-1} \cdot \omega^{-5^{\varphi'-1}}.$$

Dabei ist $\varepsilon_1 = \omega^4$, also

$$(-1, \varepsilon_1, \omega) = \omega - \omega^{-1} + \omega^{4+5} - \omega^{4-5} + \omega^{2\cdot 4+5^2} - \omega^{2\cdot 4+5^2} + - \ldots + \omega^{(\varphi'-1)4+5^{\varphi'-1}} - \omega^{(\varphi'-1)4-5^{\varphi'-1}}.$$

Setzt man für ω wieder überall $(1 - \pi)$ ein, so bekommt man

$$(-1, \varepsilon_1, \omega) = \begin{cases} - \left\{ \sum_{k=0}^{\varphi'-1} \binom{4k+5^k}{0} - \sum_{k=0}^{\varphi'-1} \binom{4k-5^k}{0} \right\} \\ - \pi \cdot \left\{ \sum_{k=0}^{\varphi'-1} \binom{4k+5^k}{1} - \sum_{k=0}^{\varphi'-1} \binom{4k-5^k}{1} \right\} \\ + \pi^2 \cdot \left\{ \sum \binom{4k+5^k}{2} - \sum \binom{4k-5^k}{2} \right\} \cdot \\ \pm \\ \vdots \end{cases},$$

also eine Zahl, deren allgemeine Ziffer lautet

$$(-1)^h \sum_{k=0}^{\varphi'-1} \binom{4k+5^k}{h} - (-1)^h \sum_{k=0}^{\varphi'-1} \binom{4k-5^k}{h}.$$

Wir wollen nun, ehe wir an die Behandlung des allgemeinen Falles gehen, die beiden Fälle $v=3$ und $v=4$ erledigen, die sich in den allgemeinen Beweis nicht einfügen, übrigens aber dasselbe Resultat ergeben.

Für $v=3$ ist die allgemeine Ziffer

$$\sum_{k=0,1} \binom{4k+5^k}{h} - \sum_{k=0,1} \binom{4k-5^k}{h} = 2 \cdot \left\{ \binom{1}{h} - \binom{7}{h} \right\}.$$

Für jedes h ist also die Ziffer durch 2 teilbar. Es handelt sich also darum, festzustellen, welches das erste h ist, für welches die Ziffer durch keine höhere Potenz von 2 teilbar ist. Das ist $h=2$. Hier ist $2 \sim \pi^4$, also $(-1, \varepsilon_1, \omega)$ durch π^6 teilbar und

$$(-1, \varepsilon, \omega) \sim \mathfrak{P}^6.$$

Für $v=4$ ergibt sich

$$\left\{ \sum_{k=0}^{3} \binom{4k+5^k}{h} - \sum_{k=0}^{3} \binom{4k-5^k}{h} \right\} = 2\binom{1}{h} + 2\binom{9}{h} - 4\binom{15}{h}.$$

Die erste nur durch 2 teilbare Ziffer bekommt man für $h=8$. Man erhält

$$(-1, \varepsilon, \omega) \sim \mathfrak{P}^{16}.$$

Wir hatten oben die allgemeine Ziffer der π-adischen Entwicklung von $(-1, \varepsilon_1, \omega)$ aufgestellt. Bezeichnen wir darin den ersten Summanden abkürzend durch Σ_h, den zweiten durch S_h, so können wir die Resolvente als Summe zweier π-adischer Zahlen schreiben:

$$(-1, \varepsilon_1, \omega) = \Sigma_0 + \pi \cdot \Sigma_1 + \pi^2 \cdot \Sigma_2 + \ldots - \left\{ S_0 + \pi \cdot S_1 + \pi^2 \cdot S_2 + \ldots \right\},$$

oder, wenn wir uns der Bezeichnung des Abschnitt II bedienen wollen,

$$(-1, \varepsilon_1, \omega) = C_1 - C_2.$$

Von der zweiten Zahl, C_2, werden wir wieder nachweisen können, dass sie verschwindet, sobald $v \geqq 5$ ist.

§ 4. Reduktion der π-adischen Entwicklung von $(-1, \varepsilon_1, \omega)$.

Wir wenden uns zur Untersuchung der Zahl C_2, deren allgemeine Ziffer

$$(-1)^{\sum_{k=0}^{\varphi'-1}} \binom{4k - 5^k}{h}$$

ist. Es ist

$$5^k - 4k = 1 + \binom{k}{2} 4^2 + \binom{k}{3} 4^3 + \binom{k}{4} 4^4 + \ldots \qquad (2)$$

$$= 1 + k \cdot 2^3 (a_0 + a_1 2^3 + \ldots)$$

Aus dieser Beziehung sieht man sofort, dass modulo 2^v sich für $k + 2^{v-3}$ immer derselbe Wert $5^k - 4k$ ergibt wie für k. Jeder solche Wert kommt also sicher schon zweimal vor. Wir wollen nun zeigen, dass sich für jedes beliebige, aber feste k_1 der Wert $5^{k_1} - 4k_1$ auch noch für ein bestimmtes k zwischen k_1 und $k_1 + 2^{v-3}$ ergibt. Dieses k unterscheidet sich von k_1 immer um eine ungerade Zahl. Es gibt für jedes k_1 eine und nur eine ungerade Zahl u zwischen 0 und 2^{v-3} so, dass $k_1 + u$ immer denselben Wert liefert wie k_1. Wir zeigen zunächst, dass zu jeder ungeraden Zahl u zwischen 0 und 2^{v-3} immer zwei Werte k gehören. Aus der Congruenz

$$4k - 5^k \equiv 4(u + k) - 5^{u+k} \mod 2^v$$

folgt

$$5^k (5^u - 1) \equiv 4u \mod 2^v,$$

und es ergibt sich weiterhin eine Congruenz als notwendige und hinreichende Bedingung, welche sich auf die Form

$$1 \equiv 5^k \cdot 5^i \mod 2^{v-2}$$

bringen lässt, und modulo 2^{v-2} gibt es ja immer genau zwei Werte k zwischen 0 und 2^{v-3}, welche diese Congruenz erfüllen.

Nun könnte die Möglichkeit bestehen, dass zu einem k zwei verschiedene Werte u existieren, so, dass für $k + u$ derselbe Wert $5^k - 4k$ wiederkehrt. Dann müsste zu zwei verschiedenen u dasselbe k gehören. Versucht man aber einen derartigen Ansatz, so wird man auf eine Unmöglichkeit der Form $1 \equiv 5^k (-5^i) \mod 4$ geführt. Nun ist die Anzahl der ungeraden Zahlen u zwischen 0 und 2^{v-3} genau 2^{v-4}. Die Anzahl aller Zahlen k von 0 bis $2^{v-3} - 1$ ist gerade doppelt so gross; und da zu jedem u genau zwei verschiedene k gehören, so ist damit bewiesen, dass zu jedem k ein und nur ein u gehört, dass also jedes $4k + 5^k$ für die Werte $k = 0$ bis $k = 2^{v-3} - 1$ mindestens zweimal vorkommt. Es kommt aber auch nur zweimal vor. Denn für eine Zahl $k + g$, wo g eine gerade Zahl bedeutet, kann ein Wert $4k + 5^k$ niemals wiederkehren, solange $g \not\equiv 0 \mod 2^{v-3}$ ist. Versucht man einen derartigen Ansatz, so wird man auf eine Unmöglichkeit der Form $1 \equiv 5^k \cdot (4n - 1) \mod 4$ geführt.

Wir kommen zum Resultat: Es kommt jeder überhaupt auftretende Wert $4k - 5^k$ genau 4 Male vor. Es müssen also genau $\frac{1}{4} \cdot 2^{v-2} = 2^{v-4}$ verschiedene Werte $4k - 5^k$ vorkommen. Nun sind die Zahlen $4k - 5^k$ alle von der Form $16n - 1$. Andererseits gibt es modulo 2^v nur 2^{v-4} verschiedene Zahlen $16n - 1$. Also müssen die Zahlen $4k - 5^k$ mit diesen

übereinstimmen. Es ist also

$$\sum_{k=0}^{\varphi'-1}\binom{4k-5^k}{h} = 4\cdot\sum_{n=1}^{2^{\nu-4}}\binom{16n-1}{h}$$

$$= 4\cdot\left\{\binom{15}{h}+\binom{31}{h}+\binom{47}{h}+\ldots+\binom{2^\nu-1}{h}\right.$$

Nun können wir aber eine Zahl angeben, deren π-adische Entwicklung gerade diese allgemeine Ziffer hat, und welche andrerseits verschwindet. Es ist das die Zahl

$$4\cdot\left\{\omega^{15}+\omega^{31}+\omega^{47}+\ldots\omega^{2^\nu-1}\right\}.$$

Sie hat die allgemeine Ziffer $4\cdot\sum_{n=1}^{2^{\nu-4}}\binom{16n-1}{h}$, wie man durch Substitution von $\omega = 1-\pi$ erkennt, und andrerseits ist der Ausdruck offenbar null für jedes $\nu>4$. C_2 verschwindet also, und es ist

$$(-1,\ \varepsilon_1,\ \omega) = C_1 = \Sigma_0 + \pi\cdot\Sigma_1 + \pi^2\cdot\Sigma_2 + \ldots.$$

§ 5. Der Ausdruck $(-1,\ \varepsilon_1^{-1},\ \omega)$.

Betrachten wir jetzt andrerseits den Ausdruck

$$(-1,\ \varepsilon_1^{-1},\ \omega) = \omega-\omega^{-1}+\varepsilon_1^{-1}\cdot\omega^5-\varepsilon_1^{-1}\omega^{-5}+\varepsilon_1^{-2}\cdot\omega^{5^2}$$
$$-\varepsilon_1^{-2}\cdot\omega^{-5^2}+-\ldots+\varepsilon_1^{-(\varphi'-1)}\omega^{5^{\varphi'-1}}-\varepsilon_1^{-(\varphi'-1)}\omega^{-5^{\varphi'-1}}.$$

$$= \sum_{k=0}^{\varphi'-1}(\omega^{-4k+5^k}-\omega^{-4k-5^k}).$$

Ersetzen wir ω^{-1} durch die Bezeichnung ω_{-1}, so kommt

$$(-1,\ \varepsilon_1^{-1},\ \omega) = \sum_{k=0}^{\varphi'-1}(\omega_{-1}^{4k-5^k}-\omega_{-1}^{4k+5^k}).$$

Man sieht jetzt schon: $-(-1, \varepsilon_1^{-1}, \omega)$ hat dieselbe Entwicklung in π_{-1}, wie $(-1, \varepsilon_1, \omega)$ in π. Es ergibt sich also

$$-(-1, \varepsilon_1^{-1}, \omega) = \Sigma_0 + \pi_{-1} \cdot \Sigma_1 + \pi_{-1}^2 \Sigma_2 + \ldots,$$

wo die Σ_i die oben angegebene Bedeutung haben.

Da die $\pi_{\pm i}$ alle untereinander äquivalent sind, enthält also $(-1, \varepsilon_1^{-1}, \omega)$ dieselbe Potenz von π wie $(-1, \varepsilon_1, \omega)$.

§ 6. Das Resultat.

Die allgemeine Ziffer $\Sigma_h = \sum_{k=0}^{\varphi'-1} \binom{4k+5^k}{h}$ lässt sich nun noch etwas anders schreiben. Es ist

$$\sum_{k=0}^{2^{\nu-2}-1} \binom{4k+5^k}{h} = 4 \cdot \sum_{k=0}^{2^{\nu-4}-1} \binom{4k+5^k}{h}.$$

Denn die Ausdrücke $4k+5^k$ sind ja, als ursprüngliche Exponenten von ω, nur modulo 2^ν zu betrachten, und es ist stets

$$4k+5^k \equiv 4(k+2^{\nu-4}) + 5^{k+2^{\nu-4}} \mod 2^\nu,$$

wie man durch die Substitution $5 = 4+1$ erkennt. Es ist also

$$(-1, \varepsilon_1, \omega) = 4 \cdot \sum_{h=0}^{\infty} (-\pi)^h \sum_{k=0}^{2^{\nu-4}-1} \binom{4k+5^k}{h}$$

$$= 4 \cdot \sum_{k=0}^{2^{\nu-4}-1} \omega^{4k+5^k},$$

und entsprechend

$$(-1, \varepsilon_1^{-1}, \omega) = -4 \cdot \sum_{k=0}^{2^{\nu-4}-1} \omega^{-4k-5^k}.$$

Daraus bekommt man die in dem Produkt

$$(-1, \varepsilon_1, \omega)(-1, \varepsilon_1^{-1}, \omega)$$

enthaltene Potenz von π durch einfache Ausmultiplikation.

Es kommt

$$(-1,\ \varepsilon_1,\ \omega)(-1,\ \varepsilon_1^{-1},\ \omega)$$
$$= -16 \cdot \sum_{h=0}^{2^v\ 4-1} \sum_{k=0}^{2^v\ 4-1} \omega^{4(k-h)+5^h(5^{k-h}-1)},$$

$$(-1,\ \varepsilon_1,\ \omega)(-1,\ \varepsilon_1^{-1},\ \omega) = -16 \cdot \sum_{i\ 0}^{2^{v-4}-1} \omega^{4i} \sum_{k-0}^{2^{v-4}-1} \omega^{5^h(5^i-1)}.$$

Hat $5^i - 1$ einen festen Wert, ist also etwa $\omega^{5^i-1} = \overline{\omega}$, so bestimmt die Reihe $\overline{\omega}^{5^h}$ jede vierte aus der Reihe der Einheitswurzeln $\overline{\omega}$. Es ist $\Sigma\overline{\omega}^{5^h}$ nur dann von null verschieden, wenn für jedes h $\overline{\omega}^{5^h}$ denselben Wert ergibt, d. h. es muss ω eine 4te Einheitswurzel sein. Das ist hier nur für den einzigen Wert $i = 0$ der Fall, und daraus ergibt sich sofort

$$(-1,\ \varepsilon_1,\ \omega)(-1,\ \varepsilon_1^{-1},\ \omega) = -2^v.$$

Also ist

$$(-1,\ \varepsilon,\ \omega) \sim \mathfrak{P}^{v \cdot 2^{v-2}} \sim 2^{\frac{v}{2}}.$$

Abschnitt IV.

Die Resolvente der Gleichung $x^m - 1 = 0$.

Es sei

$$m = 2^u \cdot p^v \cdot q^w \ldots . r^t$$

eine beliebige zusammengesetzte Zahl, worin 2, p, q, ..., r die einzelnen von einander verschiedenen Primfaktoren seien. Seien v, w, ..., t beliebige positive ganze Zahlen und sei u, um den allgemeinsten Fall herauszugreifen, — wie die andern Fälle zu behandeln sind, sieht man ohne weiteres, — sei also $u \geqq 3$ angenommen, sonst auch beliebig.

Wir betrachten die Lagrange'sche Resolvente der Gleichung

$$x^m - 1 = 0.$$

Man erhält diese folgendermassen: Seien die $\frac{1}{2}\varphi(m)$ ten Einheitswurzeln, — wenn $m \not\equiv 0 \bmod 2$, sind die $\varphi(m)$ ten zu nehmen, — durch ε_i bezeichnet. Bezeichnen wir ferner die $\varphi(m)$ primitiven m ten Einheitswurzeln durch $\omega_{\pm i}$ für $i = 1, 2, 3, \ldots, \frac{1}{2}\varphi(m)$, so erhalten wir die Lagrange'sche Resolvente, wenn wir die Summe aller Produkte $\pm \varepsilon_i \cdot \omega_{\pm i}$ bilden, wobei jedes $\pm \varepsilon_i$ dem $\omega_{\pm i}$ auf eine bestimmte Weise eindeutig zugeordnet ist,

$$(-1, \varepsilon, \omega) = \varepsilon_1 \omega_1 - \varepsilon_1 \omega_{-1} + \varepsilon_2 \omega_2 - \varepsilon_2 \omega_{-2} + \varepsilon_3 \omega_3 - \varepsilon_3 \omega_{-3}$$
$$+ - \ldots + \varepsilon_{\frac{1}{2}\varphi(m)} \omega_{\frac{1}{2}\varphi(m)} - \varepsilon_{\frac{1}{2}\varphi(m)} \omega_{-\frac{1}{2}\varphi(m)}.$$

Die eindeutige Zuordnung zwischen den ε und den ω besteht nun folgendermassen:

Es sei

α eine primitive Wurzel der Gleichung $x^{2^{u-2}} - 1 = 0$,

γ $x^{\varphi(p^v)} - 1 = 0$,

β $x^{\varphi(q^w)} - 1 = 0$,

$\vdots$

δ $x^{\varphi(r^t)} - 1 = 0$.

Dann haben wir eine primitive Wurzel ε der Gleichung $x^{\frac{1}{2}\varphi(m)} - 1 = 0$ in dem Ausdruck

$$\varepsilon = \alpha \cdot \beta \cdot \gamma \ldots \delta.$$

Alle Produkte $\alpha \cdot \beta \cdot \gamma \ldots \delta$ sind alle Wurzeln ε_i.

Ferner ist

5 eine primitive Wurzel der Congruenz $x^{2^{u-2}} - 1 \equiv 0 \bmod 2^u$

und es sei

g_p eine primitive Wurzel der Congruenz $x^{\varphi(p^v)} - 1 \equiv 0 \mod p^v$,

g_q $x^{\varphi(q^w)} - 1 \equiv 0 \mod q^w$,

$\vdots$

g_r $x^{\varphi(r^t)} - 1 \equiv 0 \mod r^t$.

Ferner sei

ζ eine primitive Wurzel der Gleichung $x^{2^u} - 1 = 0$,

η $x^{p^v} - 1 = 0$,

ϑ $x^{q^w} - 1 = 0$,

$\vdots$

ξ $x^{r^t} - 1 = 0$.

Dann haben wir alle primitiven Wurzeln dieser Gleichungen beziehungsweise in den Formen

$$\zeta^{\pm 5^h},\ \eta^{g_p^i},\ \vartheta^{g_q^k},\ \ldots,\ \xi^{g_r^l},$$

und wir haben also alle primitiven Wurzeln ω der Gleichung $x^m - 1 = 0$ in der Form

$$\zeta^{\pm 5^h} \cdot \eta^{g_r^i} \cdot \vartheta^{g_q^k} \ldots \xi^{g_r^l}.$$

Haben wir nun ein bestimmtes $\pm \varepsilon$, etwa

$$\pm \varepsilon_i = \pm\ \alpha^a \cdot \beta^b \cdot \gamma^c \ldots \delta^d,$$

so wollen wir als $\omega_{\pm i}$ das folgende bezeichnen

$$\omega_{\pm i} = \zeta^{\pm 5^a} \cdot \eta^{g_p^b} \cdot \vartheta^{g_q^c} \ldots \xi^{g_r^d},$$

und dieses $\omega_{\pm i}$ ist dem $\pm \varepsilon_i$ eindeutig zugeordnet. Es ist dann unsere Resolvente

$$(-1, \varepsilon, \omega) = \sum_{h,\ i,\ k,\ \ldots,\ l} \pm \alpha^h \beta^i \gamma^k \ldots \delta^l \cdot \zeta^{\pm 5^h} \eta^{g_p^i} \vartheta^{g_q^k} \ldots \xi^{g_r^l}.$$

Dieses ist die Lagrange'sche Resolvente, welche die Gleichung $x^m - 1 = 0$ auflöst. Mit Hilfe dieser Gleichung sieht man aber sofort: Es ist

$$(-1, \varepsilon, \alpha,) = (-1, \alpha, \zeta) \cdot (\beta, \eta) \cdot (\gamma, \vartheta) \ldots (\delta, \xi),$$

und da wir diese einzelnen Resolventen in den Abschnitten I, II und III schon in ihre Primfaktoren zerlegt haben, so ist unsere Aufgabe erledigt.

Lebenslauf.

Ich, Paul Friedrich Karl Berger, evangelischer Konfession und preussischer Staatsangehörigkeit, wurde am 18ten Januar 1890 in Krefeld (Rheinland) geboren, als Sohn des Kaufmanns Paul Berger und seiner † Frau Luise geb. Graas. Vom 6ten bis zum 9ten Lebensjahr besuchte ich die Elementarschule meines Heimatsortes, dann das dortige Realgymnasium, an welchem ich Ostern 1908 die Reifeprüfung bestand. Ich studierte dann in Heidelberg (S.-S. 1908 und W.-S. 1908/9), Bonn (S.-S. 1909), Leipzig (W.-S. 1909/10) und Marburg (S.-S. 1910 bis jetzt). Das Rigorosum bestand ich am 4ten Juni 1913.

Von meiner früheren Studienzeit her glaube ich besonders den Herren Professoren Geheimrat Koenigsberger (Heidelberg) und Geheimrat Study (Bonn) zu Dank verpflichtet zu sein, von meiner Marburger Studienzeit her den Herren Professoren Hensel, v. Dalwigk, Neumann, Richarz, Feussner, Schulze, Natorp, Cohen.

Vor allem möchte ich aber auch an dieser Stelle nochmals Herrn Geh. Reg.-Rat Prof. Dr. Hensel meinen herzlichsten Dank aussprechen, der mir bei der Abfassung der Arbeit Rat und Hilfe in gütigster Weise hat zu Teil werden lassen.